15

CONDUTAS PERPETRADAS POR CIVIS PELO CIBERESPAÇO NO CURSO DOS CONFLITOS ARMADOS ENTRE ESTADOS – O CASO DA UCRÂNIA

Alexandre Peres Teixeira*

Resumo: O estudo dos efeitos da guerra cibernética em jurisdições nacionais já está emergindo como um tópico relevante para a Academia. O fenômeno do "Exército de TI" ucraniano demonstrou a possibilidade de ampla participação de civis, das mais diversas partes do mundo, na realização de ataques cibernéticos, no contexto de conflitos armados. O envolvimento de civis não autorizados em condutas bélicas afeta o principal paradigma do Direito Internacional Humanitário, relacionado ao *Jus in Bello*, representando um grande desafio ao escopo de proteção que o Direito Internacional Humanitário (DIH) atribui aos civis que não participam do conflito. As peculiaridades do ciberespaço permitem que indivíduos vinculados às mais diversas jurisdições do planeta se envolvam em condutas que, de acordo com o direito da guerra, somente combatentes poderiam realizar. Este artigo analisará os seguintes tópicos: a formação e as ações do "Exército de TI" ucraniano e sua aderência à lei; o envolvimento de civis em hostilidades cibernéticas e as implicações jurídicas destas condutas. Busca-se trazer para a discussão acadêmica, em nível nacional, o debate sobre as consequências jurídicas do uso das novas tecnologias por civis em conflitos armados.

Palavras-chave: Ciberespaço. Conflito Armado. Direito Internacional Humanitário. Jurisdição Nacional.

Sumário: 1. Introdução. 2. Ciberespaço: porta aberta para o engajamento de civis em conflitos armados. 2.1. Hackers civis no front do conflito armado cibernético. 2.2. Civis comuns na linha tecnológica de fogo. 3. A abordagem jurídica das ações realizadas por civis no conflito da Ucrânia –

* Doutor em Direito pelo CEUB. Mestre em Ciências Navais pela Escola de Guerra Naval. Especialista em DIH pela *Ruhr University Bochum.* Especialista em Direito Internacional Cibernético pelo Processo de Haia. Coordenador de Pesquisa e Pós-Graduação na Escola Nacional de Formação e Aperfeiçoamento de Magistrados da Justiça Militar da União, Brasília, DF. E-mail: alexandre teixeira@stm.jus.br

Conduct perpetrated by civilians through cyberspace in the course of armed conflicts between states – the case of Ukraine

Abstract: The study of the impact of cyber warfare on national jurisdictions is already emerging as a relevant topic for academics. The phenomenon of the Ukrainian "IT Army" has demonstrated the possibility of widespread participation of civilians from all over the world in conducting cyber attacks in the context of armed conflicts. The involvement of unauthorized civilians in belligerent conduct affects the main paradigm of international humanitarian law, related to jus in bello, and represents a major challenge to the scope of protection that international humanitarian law (IHL) assigns to civilians who do not participate in the conflict. The particularities of cyberspace allow individuals linked to the most diverse jurisdictions on the planet to engage in conduct that, under the laws of war, only combatants could engage in. This article analyzes the following topics: the formation and actions of the Ukrainian "IT Army" and its compliance with the law; the involvement of civilians in cyber hostilities and the legal implications of such conduct. The aim is to bring the debate on the legal consequences of the use of new technologies by civilians in armed conflicts into the academic discussion at the national level.

Keywords: Cyberspace. Armed conflict. International humanitarian law. National jurisdiction.

1 Introdução

"Por conseguinte, do ponto de vista da Cibernética, o mundo é um organismo, nem tão rígido ao ponto de que qualquer mudança em algum aspecto o faça perder sua identidade, nem tão frouxamente articulado que qualquer coisa possa acontecer."
Norbert Wiener (1956)

Em 24 de fevereiro de 2022, após o apelo público dramático do Ministro da Defesa ucraniano, Mykhailo Federov, divulgado pelas redes sociais, pelo qual solicitava que hackers de todo mundo se unissem às forças armadas ucranianas, com a finalidade de comporem um "exército digital" contra a Rússia, milhares de pessoas no mundo todo atenderam ao chamado para a guerra, dentre elas, o grupo de hackers conhecido como *Anonymous*, que fez uma declaração de guerra cibernética contra a Rússia. No seu pronunciamento, o grupo alegou que tinha como alvo as estações de TV estatais, os Ministérios do governo e os bancos

estatais. Uma série de ataques cibernéticos foi executada pelo grupo, em retaliação aos ataques cibernéticos perpetrados pela Rússia a sites e empresas do governo ucraniano.

O uso do ciberespaço como ferramenta de guerra tem mostrado efeitos imprevisíveis. Suas características *sui generis* atribuem ao domínio cibernético qualidades e vantagens que os meios e métodos convencionais não possuem. Furtividade, anonimização, possibilidade de operação remota e longínqua, flexibilidade, versatilidade e baixíssimo custo, quando comparado com os meios convencionais, fazem do ciberespaço uma opção irrecusável para seus utilizadores.

Somado a isso, a inexistência de uma normatização específica e pacífica, capaz de estabelecer critérios de governança para seus usuários. Sem nenhuma dúvida, o ciberespaço figura como uma opção militar vantajosa e letal, mas também disponível para qualquer ser humano, de qualquer parte do planeta, que queira se aventurar e tomar parte em hostilidades cibernéticas.

Sobre esta questão, Kilovaty[1] afirma que a emergência do ciberespaço como instrumento de guerra exacerba as lacunas e ambiguidades que já existem no DIH. Um fator particularmente agravante é o aumento do envolvimento de civis em ataques cibernéticos (KILOVATY, 2016).

Neste sentido, civis, em conflitos armados modernos, podem desempenhar um papel ativo quando se trata desses ataques, pois atuam como contratados privados realizando operações cibernéticas ofensivas e defensivas. Embora a noção tradicional de conflito armado inclua membros das Forças Armadas regulares ("combatentes"), esse paradigma não é mais o caso no campo de batalha moderno, devido ao crescente envolvimento de civis em hostilidades cibernéticas (KILOVATY, 2016).

A base normativa do Direito Internacional Humanitário (DIH) cibernético, ainda em processo de franca construção, estabelece que as hostilidades[2] cibernéticas, entre beligerantes, que ocorram no curso dos conflitos armados, podem ser consideradas como ações de combate gítimas, caso seus utilizadores observem os princípios consagrados do DIH (WATERMAN, 2023a).

Tais hostilidades podem se materializar, com a realização de operações maliciosas com efeitos "cibercinéticos", que busquem a causação de danos físicos, por meio dos efeitos diretos, secundários ou terciários; ou então, por ope-

1 KILOVATY, I. Virtual Violence – Disruptive Cyberspace Operations as "Attacks" Under Humanitarian Law. *Michigan Telecommunications and Technology Law Review*, Michigan, v. 23, n. 1, 2016. Disponível em: <https://repository.law.umich.edu/mttlr/vol23/iss1/3>. Acesso em: 22 set. 2023.

2 Para a conquista de uma determinada finalidade militar, tais hostilidades podem se materializar com a realização de operações cibernéticas maliciosas que gerem reflexos "cibercinéticos", que busquem a causação de danos físicos, por meio dos efeitos primários, secundários ou terciários; ou então, por operações que, apesar de não serem capazes de romperem a barreira do dano físico, causem danos lógicos que influenciem as operações militares do inimigo.

rações que, apesar de não romperem a barreira do dano físico, causem danos lógicos capazes de influenciar nas operações militares.

Para Kowalczewska (2023) o uso da força, seja cinética ou cibernética, afeta a vida cotidiana da sociedade, em níveis público e privado, levando a uma desordem tangível. Neste sentido, tanto o sistema normativo interno, pautado na Constituição, como o sistema normativo internacional, que possui como principais bases os tratados, os costumes e os princípios do direito permitem a reavaliação de prioridades e dos níveis de proteção para bens tutelados específicos, em nome da necessidade primordial que pode ser perfazer em uma emergência peculiar.

Para a autora isso inclui salvaguardar valores como segurança pública, saúde e a sobrevivência do Estado como base para derrogações das obrigações do Direito Internacional dos Direitos Humanos (DIDH) (KOWALCZEWSKA, 2023, p. 1.063).

Desta forma, visando permitir a discussão deste novo fenômeno da história das guerras no meio acadêmico brasileiro, este artigo sustenta que as novas tecnologias advindas da era da informação, ao darem acesso remoto às pessoas às hostilidades cibernéticas em conflitos armados, torna possível a realização de condutas que podem levar a violações das normas postas para a regulação dos conflitos armados entre Estados.

As perguntas de pesquisa que foram selecionadas para a sustentação da tese defendida no presente artigo são:

1. Em que medida a utilização do ciberespaço facilita a participação de civis em hostilidades cibernéticas, no curso dos conflitos armados?
2. Tendo em vista a base normativa positivada e os novos entendimentos relacionados ao uso das novas tecnologias em conflitos armados, de que forma as condutas realizadas remotamente por civis se constituem em violação das normas de Direito Internacional Humanitário?

Para se tentar obter a reposta aos questionamentos realizados acima, após esta breve introdução, este artigo seguirá o seguinte caminho: na Seção 2, será verificado se o ciberespaço pode ser considerado uma porta aberta para a inserção de civis em hostilidades cibernéticas no curso dos conflitos armados do século 21. Na Seção 3, serão abordados os aspectos jurídicos, sob o ponto de vista do DIH, da participação de civis em hostilidades cibernéticas. Ao final do artigo, será apresentada uma síntese em forma de conclusão.

A revisão da literatura para a construção do presente artigo considerou a posição doutrinária do Comitê Internacional da Cruz Vermelha (CICV); as discussões do Grupo de Especialistas que escreveram o Manual de Tallinn 2.0; as Normas Convencionais de Direito Internacional Humanitário; as Normas de Direito Internacional Consuetudinário; como também o posicionamento doutriná-

rio de autores como: Biggerstaff, W. C,Henckaerts, J. M. e Beck, L. D, Ido Kilovaty, Kaja Kowalczewska, KuboMacak, Nills Melzer e Michael N. Schmitt.

2 Ciberespaço: porta aberta para o engajamento de civis em conflitos armados

"Pequenas guerras são travadas pelas forças armadas de um país. Guerras totais são travadas por nações inteiras" (JOSHI, 2023, p. 1 – tradução nossa). Uma realidade incontestável para os conflitos armados modernos é o fato de os civis desempenharem um papel importante,[3] assim como estão desempenhando na defesa[4] da Ucrânia. Joshi (2023) afirma que, quando a *Ukrposhta*, a agência postal nacional da Ucrânia, realizou um concurso para criar um selo comemorativo, a proposta vencedora mostrava um trator civil rebocando um tanque russo capturado — uma das imagens mais icônicas da guerra.

Não é incomum para guerras totais que a distinção "civil-militar" seja normalmente rompida. No caso da Ucrânia, a sociedade tem desempenhado um papel corajoso, valente e fundamental para os rumos que o conflito tomou. Segundo Joshi (2023), os moradores, para tirar fotos, esconderam seus telefones celulares das tropas russas e revelaram a localização dos equipamentos russos, colocando alfinetes virtuais no *Google Maps.* O governo construiu um aplicativo governamental especialmente dedicado ao tema, o *"e-Verog"*, com a finalidade de oferecer, aos civis, uma maneira deles passarem informações táticas operacionais.

A conectividade e a proliferação de *smartphones*, que dependem desta conectividade, aceleraram e transformaram uma forma mais antiga de colaboração civil-militar, familiar das redes de resistência da França, ocupada na Segunda Guerra Mundial. Por algum tempo, diz o general Sir Jim Hockenhull, chefe da inteligência de defesa da Grã-Bretanha, no início da invasão, os exércitos tentaram transformar cada soldado e plataforma em um sensor.

Para Joshi (2023), o que aconteceu foi que muitas pessoas se tornaram sensores e como resultado disto se formou uma rede de sensores civis de

[3] "O coronel ucraniano Shevchuk disse que se seus homens soubessem que os russos estavam perto de uma determinada aldeia, mas não tivessem certeza de onde exatamente estavam, eles abririam o *Google Maps*, encontravam uma loja local e ligariam para ela. 'Boa noite, somos da Ucrânia! Você tem algum *kaptsaps* [russo] por aí? Sim. Onde? Onde? Atrás da casa da vovó Hanna. Que casa é essa? Bem, todo mundo a conhece!' Então você conversa um pouco com as pessoas e descobre onde está tudo" (JOSHI, 2023, p. 3).

[4] "Kiev colocou a resistência entre sociedades no coração da sua defesa nacional" mouse (SHELEST, 2022, p. 2 – tradução nossa). Bem-vindo ao admirável mundo novo da guerra cibernética, no qual qualquer pessoa, em qualquer lugar do mundo, pode participar das hostilidades de um conflito armado real, sentada em seu sofá, em uma residência confortável, com um clique teclado.

crowdsourcing, que provou ser muito importante para o contexto do conflito armado em curso (JOSHI, 2023). Em uma zona de guerra moderna, qualquer pessoa com um *smartphone* é uma fonte potencial de inteligência militar. Desde os primeiros dias da invasão russa, a Ucrânia vem coletando informações com a larga utilização de civis. Entretanto, esta ideia não é nova.

Durante a Segunda Guerra Mundial, voluntários britânicos telefonavam alertando sobre ataques aéreos. Para o conflito atual, entre Rússia e Ucrânia, em março de 2022, o Ministério de Transformação Digital da Ucrânia configurou o *chatbot "e-Vorog"* (*"e-Enemy"*), apenas algumas semanas após a invasão da Rússia. Parece ser a primeira tecnologia, para este tipo de finalidade, desenvolvida por um governo em situação de conflito armado.

Usando um *smartphone*, o *chatbot e-verog* leva os usuários a uma lista de perguntas para que seja avaliado o que viram, onde viram e quando viram e, desta forma, coletar inteligência operacional útil, para ser trabalhada e transformada em informação (THE ECONOMIST, 2023). Sem dúvidas, isto coloca o civil, que possui um status privilegiado e protegido pelo princípio internacional da proteção à pessoa humana, na alça de mira dos soldados russos, não que os russos tenham este direito. Neste sentido, o envolvimento de civis em ações de coleta de inteligência operacional[5] abre um grande debate sobre o status destas pessoas, que tomam parte em eventos como estes, aproveitando-se das peculiaridades da tecnologia.

2.1 Hackers civis no front do conflito armado cibernético

Em se tratando de conflitos da era contemporânea, a reunião entre esferas governamentais, setor privado e voluntários civis em geral, especificamente para tarefas de guerra cibernética, teve seu ápice no conflito entre Rússia e Ucrânia que se iniciou em fevereiro de 2022 com a formação do que ficou conhecido como "Exército de TI da Ucrânia". Nesse sentido, segundo Soesanto (2022, p. 4 – tradução nossa), por vários anos, antes da invasão russa, a ideia principal de se criar um exército de voluntários cibernéticos já era veiculada nos círculos do governo ucraniano. Em parte, essas discussões foram intensificadas em virtude

[5] A resistência popular habilitada digitalmente nessa escala teria sido praticamente impossível 15 anos atrás. Jack McDonald, do *King's College London*, aponta que, quando os Estados Unidos invadiram o Afeganistão em 2001, menos de 1% da população local tinha acesso à internet. Na Síria, em 2011, quando a guerra civil já estava em curso e as filmagens do combate por celulares se tornaram comuns, a taxa ainda era de apenas 22%. Quando a Rússia invadiu a Ucrânia em 2014, atingiu 46%. Quando o fez novamente no ano passado, o número disparou para quase 80%. "O que você está vendo na Ucrânia", diz ele, "é o que vai ser padrão" (JOSHI, 2023, p. 3).

do sucesso da "Unidade Cibernética da Liga de Defesa da Estônia" e outros esforços, em todo o mundo, "para organizar, incorporar e aumentar os voluntários civis, de TI, nas estruturas militares existentes, em tempos de crise".

Segundo Biggerstaff (2023), dois dias após a invasão da Rússia, em território ucraniano, o Ministro da Transformação Digital da Ucrânia anunciou, no *Twitter*, um apelo às armas digitais (BIGGERSTAFF, 2023). Para Shore (2022), o vice-primeiro-ministro, Mykhailo Fedorov, deu um passo que, provavelmente, nenhum outro funcionário de governo, no mundo, jamais deu: convocou, publicamente, *hackers* voluntários para derrubar sites de outros países. E ele tinha uma lista de 31 sites do governo russo, de bancos e corporações, pronta para usar. Em poucos dias, a Ucrânia reuniu um "exército de TI de mais de 400.000 voluntários" (SHORE, 2022, p. 1 – tradução nossa).

Mais de um ano depois, o chamado Exército de TI agregava quase 200.000 voluntários (este número já esteve perto de 310.000, no início do conflito). Esses operadores cibernéticos têm atuado contra os sites e redes de empresas civis russas, bem como contra a infraestrutura crítica da Rússia, pública e privada, por meio de várias operações cibernéticas maliciosas. Inclusive existem registros de que "[...] estes hackers usaram software de reconhecimento facial e a mídia social para notificar as famílias de soldados russos mortos" (BIGGERSTAFF, 2023, p. 1 – tradução nossa), o que pode ser considerado uma grave violação do DIH.

No bojo destas ações, Romandash (2023) acredita que os ucranianos estão minando a influência[6] digital russa, além de isolar e cortar sua a tecnologia com o resto do mundo. No início da invasão em grande escala, o ministro Mykhaylo Fedorov, também lançou uma campanha para facilitar o "bloqueio digital" da Rússia e encorajar as empresas ocidentais a tomar ações contra aquele Estado (WATERMAN, 2023a).

Segundo Waterman (2023a, p. 1 – tradução nossa), o Comitê Internacional da Cruz Vermelha (CICV) expressou, separadamente, a preocupação com a prática de "recrutar voluntários civis para participar de operações cibernéticas militares", alertando: "embora nem toda forma de envolvimento civil no campo de batalha digital se qualifique como participação direta, o perigo é que

[6] O Kremlin trava uma guerra de informação por meio de canais de propaganda, exércitos de *trolls* e "idiotas úteis" no Ocidente e além, que repetem e compartilham a propaganda russa. Antes de lançar uma invasão em grande escala rumo à Ucrânia, a Rússia manteve uma guerra de baixa escala com o país no início de 2014. Esse conflito, que culminou na anexação da península da Crimeia e na guerra do Donbass, recebeu menos atenção internacional do que a invasão de 2022. A Rússia foi capaz de controlar a narrativa sobre a situação em Donbass e na Crimeia e diminuir significativamente o apoio e o interesse pela Ucrânia de 2014 a 2022. No entanto, as coisas mudaram após o início da mais recente guerra em grande escala (ROMANDASH, 2023).

possa ser vista como tal pelo inimigo, expondo assim muitos civis a um risco de danos graves". Em resposta a essas advertências, a Ucrânia está atualmente elaborando uma lei, "com o objetivo de acabar com a incerteza sobre o status do Exército de TI" (WATERMAN, 2023a, p. 2 – tradução nossa), "incorporando formalmente seus membros ao componente de reserva de suas forças armadas" (BIGGERSTAFF, 2023, p. 1 – tradução nossa).

O Exército de TI da Ucrânia está trabalhando para fortalecer a capacidade do país, a se proteger de ataques cibernéticos russos e a aumentar a segurança da sua infraestrutura digital, visto que o país melhorou, significativamente, sua resistência às ameaças cibernéticas russas (ROMANDASH, 2023). De acordo com especialistas militares ocidentais, a Ucrânia foi capaz de realizar "uma verdadeira revolução ao se elevar ao mercado em sua luta cibernética defensiva" (BASSO, 2023).

Para Romandash (2023), um dos principais ganhos do Exército de TI foi combater, com sucesso, a guerra psicológica empreendida pela Rússia, contra a Ucrânia, desde 2014. Desta forma, a autora acredita que em 2022 a Ucrânia mudou a visão internacional sobre a invasão russa. Neste sentido, os esforços da Ucrânia contribuíram, significativamente, para o isolamento digital da Rússia e integraram as narrativas da Ucrânia, com a ajuda de dados de fontes abertas, aliados digitais e campanhas de comunicação bem-sucedidas (ROMANDASH, 2023).

É igualmente claro que o Exército de TI está atacando, de forma persistente e indiscriminada, a infraestrutura civil russa, incluindo farmácias on-line, bancos, serviços de entrega de alimentos e varejistas. A conduta do grupo interno do Exército de TI evoluiu rapidamente, de meras desfigurações de sites russos, durante os primeiros dias da invasão, para campanhas de espionagem sofisticadas. Evoluiu também para a primeira operação cibernética ofensiva destrutiva – que visou uma plataforma de vídeo civil – no início de maio 2022.

Outro emprego dos hackers civis do "Exército de TI ucraniano" se dá no front da guerra cognitiva, pois é a Rússia contumaz na realização de campanhas de guerra cognitiva contra seus adversários geopolíticos, inclusive em tempos de paz. As capacidades russas para a guerra cognitiva dependem da tecnologia ocidental, bem como de recursos financeiros para financiar inúmeras fábricas de *trolls*, *hackers* e "idiotas úteis".[7] Redes de "lobistas" russas tentam "espalhar as narrativas da Rússia em países ao redor do mundo" (ROMANDASH, 2023, p. 5 – tradução nossa).

Para tentar combater a campanha de desinformação russa, no conflito em curso, a Ucrânia fez parceria com empresas de tecnologia como a *Clearview* e

[7] Figuras públicas relativamente influentes que promovem mensagens favoráveis ao Kremlin no contexto local em troca de pagamentos da Rússia (ROMANDASH, 2023).

a *Palantir*, dos EUA, que fornecem soluções, baseadas em IA, às questões de identificação com biometria facial, bem como para a tomada de decisões táticas, na linha na frente de combate (SCOTT, 2022).

Por meio dessa parceria, as Forças Armadas da Ucrânia podem acessar dados que identificam melhor os soldados da Rússia, e usar essas informações, com o emprego do Exército de TI, para sua própria guerra de informação com a finalidade de resistir à campanha de guerra cognitiva da Rússia. O *software* adquirido combina a imagem real de soldados russos, cometendo crimes de guerra, e mostrando *on time* as suas identidades. Com certeza uma tecnologia que será extremamente útil para futuros tribunais de guerra (LONAS, 2022).

À medida que aumenta o número de mortos na guerra entre a Rússia e a Ucrânia, a questão de como tratar adequadamente os restos mortais de soldados mortos tornou-se um tema recorrente. Alguns relatos da mídia afirmam, por exemplo, que as forças armadas ucranianas também estão utilizando o "Exército de TI" para publicar fotos de soldados russos mortos nas redes sociais para que os familiares possam "determinar se as imagens apresentam um ente querido desaparecido" (BIGGERSTAFF, 2022). Segundo Brewster (2022), a orientação do governo ucraniano, em relação a esta questão é a seguinte:

> Encontre uma foto de um soldado russo morto, nas redes sociais. Carregue-o no software de reconhecimento facial. Obtenha uma correspondência de identidade de um banco de dados de bilhões de imagens de mídia social. Identifique a família e os amigos do falecido. Mostre a eles o que aconteceu com a vítima da guerra de Putin contra a Ucrânia (BREWSTER, 2022, p. 2 – tradução nossa).

Autoridades[8] ucranianas realizaram mais de 8.600 buscas de reconhecimento facial em soldados russos mortos ou capturados nos 50 dias desde o início da invasão, usando as varreduras de IA para identificar corpos e contatar centenas de famílias, no que pode ser uma das aplicações mais horríveis da tecnologia no curso de um conflito armado. Os ativistas cibernéticos do "Exército de TI da Ucrânia" dizem que usaram essas identificações para informar as famílias sobre a morte de 582 russos, inclusive enviando-lhes fotos dos cadáveres abandonados, que são postadas em redes sociais (HARWELL, 2022).

O governo ucraniano defende o uso do software de escaneamento facial da empresa de tecnologia norte-americana *Clearview AI*, afirmando que se trata de uma forma brutal, mas eficaz, de provocar dissidência dentro da Rússia, desencorajar outros combatentes e apressar o fim de uma guerra devastadora. Contudo, alguns analistas militares e de tecnologia temem que a estratégia possa

[8] Os funcionários da *Clearview AI* agora realizam chamadas de treinamento semanais, às vezes diárias, pelo *Zoom* com novos oficiais da polícia e militares que desejam obter acesso. O sistema foi usado principalmente por policiais e investigadores federais, nos Estados Unidos, para verificar se uma foto de um suspeito ou testemunha correspondia a qualquer outra, em seu banco de dados, de 20 bilhões de imagens, tiradas de mídias sociais e da Internet pública (HARWELL, 2022).

sair pela culatra, inflamando a raiva na sociedade russa por uma campanha de choque e pavor dirigida a mães e esposas, que podem estar a milhares de quilômetros daqueles que realmente decidem sobre a máquina de guerra do Kremlin (HARWELL, 2022).

Esta tem sido uma das estratégias de guerra psicológica da Ucrânia para tentar informar os russos sobre a morte de familiares, aos quais, supostamente, o acesso à mídia é controlado pelo governo. Segundo o governo da Ucrânia, as informações sobre mortes que têm sido causadas pela insana invasão autorizada pelo Presidente Putin não podem ser controladas pela Federação russa.

Brewster (2022) afirma que o Ministro Mykhailo Fedorov, confirmou, em seu perfil no *Telegram*, que a tecnologia de vigilância estava sendo usada dessa maneira, semanas depois que a *Clearview AI*, empresa provedora de reconhecimento facial, com sede em Nova Iorque, passou a oferecer seus serviços à Ucrânia para os mesmos fins (BREWSTER, 2022). A *Clearview AI* estaria fornecendo seu software, gratuitamente, ao governo ucraniano.

Em entrevista à Reuters, o CEO da *Clearview*, Hoan Ton-That, disse que a empresa tinha um estoque de 10 bilhões de rostos de usuários, extraídos de mídias sociais, incluindo dois bilhões do *Facebook* russo, que é chamado de *"Vkontakte"*. Fedorov escreveu em um post no *Telegram* que o objetivo final era "dissipar o mito russo de uma 'operação especial' cirúrgica, na qual 'não há recrutas' e 'ninguém morre" (BREWSTER, 2022, p. 1 – tradução nossa).

Contudo, a sinistra conduta dos ucranianos demonstra para os defensores da privacidade que devem se preocupar com o uso da biometria facial em tempos de conflitos armados, principalmente quando isso puder legitimar o uso da tecnologia em outros cenários, nos quais a privacidade dos vivos estiver ameaçada (BREWSTER, 2022), como no caso da privacidade da família do soldado morto em combate, cuja foto passa a ser exposta em uma rede social pública. Para o Estado ucraniano, não obstante as questões ético-jurídicas, acredita-se que seja necessário identificar soldados russos mortos, pois, segundo alegam, existe muita controvérsia sobre o número de militares russos falecidos, por conta da guerra de narrativas que se passa em paralelo com as hostilidades ativas.

O fenômeno do Exército de TI da Ucrânia figura como um dos maiores desafios, atualmente, para o Direito Internacional. Não apenas em razão da dificuldade de se estabelecer um status jurídico para os membros do suposto grupo de *hackerse* voluntários civis em geral que o compõem, mas também porque o fenômeno denuncia a dificuldade do direito posto, tanto interno como internacional, que foi construído sob paradigmas extremamente diferentes, em se adaptar às sensíveis nuances da guerra cibernética, que afrontam a soberania, a territorialidade, a humanidade e a privacidade.

2.2 Civis comuns na linha tecnológica de fogo

Outra questão preocupante, em relação ao chamado do governo ucraniano para que a sociedade se envolvesse na defesa do país está relacionada com o envolvimento de civis em geral, nas ações cibernéticas, que mesmo sem possuírem capacidade técnica apurada para atuarem nas operações maliciosas executadas contra ativos cibernéticos russos. Existe uma considerável parcela da sociedade ucraniana que atua na coleta de inteligência operacional, com a utilização do *Appe-Vorog*, um aplicativo criado pelo governo ucraniano para a coleta de dados sobre movimentações de tropas russas.

Na porção da Ucrânia ainda não ocupada por tropas russas, os civis têm usado o *e-Vorog* para relatar a localização de bombas não detonadas e outras munições. Neste mesmo sentido, outro aplicativo, o *Eppo*, permite que seus usuários gravem o voo de aeronaves, mísseis e drones. Mísseis balísticos, que viajam alto e rápido, não podem ser facilmente rastreados por civis. No entanto, o *Shahed-136*, um drone armado fabricado pelo Irã, que tem sido usado pelos russos para atacar a infraestrutura ucraniana, navega lentamente em baixa altitude e é frequentemente avistado (THE ECONOMIST, 2023).

Informações enviadas por meio do aplicativo *Eppo* ajudam caças ucranianos a abaterem estes drones. O mesmo aplicativo também é usado para alertar as equipes que utilizam armas antimísseis (THE ECONOMIST, 2023). Em setembro de 2022, moradores da cidade de Kherson, então sob controle russo, usaram o *e-Verog* para relatar a localização de um depósito, onde veículos militares russos foram armazenados. O prédio foi destruído por um forte ataque no dia seguinte. Prédios usados como quartéis, na região, também foram atingidos.

Ressalta-se que colaboradores dos russos também usaram aplicativos, disfarçados de jogos em celulares, para registrar os movimentos da artilharia ucraniana (THE ECONOMIST, 2023). E, desta forma, as novas tecnologias vão sendo inseridas no contexto das hostilidades de conflitos armados, criando uma dependência perigosa, que envolve população civil e desconstrói bases paradigmáticas que sustentam o direito da guerra, principalmente a proteção de civis.

Fato é que as pessoas que enviam informações, via *e-Vorog*, de áreas ocupadas pela Rússia correm grandes riscos. O próprio aplicativo possui um tutorial que aconselha aos usuários a excluírem de seus telefones qualquer evidência[9] de que tenham carregado algum dado operacional. A população civil que

[9] Em 2020, houve um grande vazamento de informações pessoais do banco de dados de carteira de habilitação da Ucrânia. O *Diia*, o aplicativo usado para verificar os usuários do *e-Vorog*, também armazena as carteiras de motorista digitais. Funcionários negaram que o vazamento estivesse ligado a *Diia*. Mas se informações de identificação semelhantes para usuários do *e-Vorog* fossem descobertas pelos serviços de inteligência russos, isso poderia ser uma sentença de morte para os informantes (THE ECONOMIST, 2023).

se envolve na coleta de inteligência operacional enfrenta constantes represálias das tropas russas e alguns civis já foram mortos por conta desta atividade extremamente perigosa.

Neste sentido, para o senso comum castrense, o repasse de informações táticas para um dos beligerantes pode se configurar em coleta de dados de inteligência, o que pode ser considerado como Participação de Civis nas Hostilidades (DPH). Adotando tal conduta o civil perde, ainda que temporariamente, a proteção contra os ataques diretos das tropas russas (THE ECONOMIST, 2023).

Joshi (2023) argumenta que uma lição para ser extraída desta situação peculiar é que a conectividade se torna, cada vez mais, um recurso militar vital. Há muito tempo, o Talibã derrubou torres de telefonia móvel para impedir que aldeões afegãos enviassem denúncias às forças de segurança. Os cartéis de drogas mexicanos agora usam equipamentos de interferência de sinal. Segundo Joshi, o general Nikolyuk, da Ucrânia, afirmou que a assistência civil foi menos disponível em Kharkiv e Donetsk, no Leste, porque a Rússia interrompeu as redes de telefonia móvel nessas áreas (JOSHI, 2023).

Tudo isso ocorre sob o pressuposto de que os exércitos estão fazendo esforços de boa-fé para discriminar civis de soldados – isto é, que eles se preocupam com as leis da guerra. Se os civis ucranianos frequentemente estão dispostos a comprometer seu status de não combatentes, atuando como sensores de Inteligência para as tropas ucranianas, pode motivar o exército da Rússia no sentido de demonstrar pouca consideração pelos civis ucranianos.

Segundo Romandash (2023), os dados de fontes abertas foram cruciais para fornecer evidências dos crimes cometidos pelo exército russo em Bucha, Borodyanka e outros territórios liberados da Ucrânia. A autora segue afirmando que este tipo de inteligência está sendo empregada, ativamente, enquanto a guerra continua "com a finalidade de ajudar a localizar, geograficamente, as tropas russas, confirmar declarações sobre batalhas importantes e descobrir locais de onde mísseis estão sendo lançados contra a Ucrânia" (ROMANDASH, 2023, p. 6 – tradução nossa).

Neste contexto, a realidade fática que acompanha o conjunto de condutas observadas no caso concreto em comento envolve princípios caros para o DIH, como o Princípio da Distinção, o Princípio da Humanidade e o Princípio da Proporcionalidade. Neste sentido, as violações do DIH presentes nas referidas condutas podem dar motivação para o enquadramento das supostas condutas em crimes da competência material do Tribunal Penal Internacional (TPI), principalmente no tipo penal do crime de guerra, que no caso em comento, pode ser o crime de maior incidência, ainda que cometidos por civis.

3 A abordagem jurídica das ações realizadas por civis no conflito da Ucrânia – a participação Direta de Civil em Hostilidades (DPH)

Coletivos de hackers são empregados como representantes de Estados há muito tempo, tanto em épocas de paz como de guerra. Basta verificar os casos abordados até aqui. Notavelmente, os *hacktivistas* patrióticos russos atacaram a Estônia em 2007, a Geórgia em 2008, sendo que na Georgia, também em uma situação de conflito armado, assim que os tanques russos chegaram à cidade. Entretanto, a Ucrânia é o primeiro país, e certamente a primeira democracia europeia, a abraçar abertamente uma milícia de *hacktivistas* durante um conflito armado real, o que levanta questões legais complexas e difíceis de serem abordadas (WATERMAN, 2023b).

Como o Exército de TI se declara independente das forças armadas ucranianas e seus voluntários não usam uniforme, eles, neste momento do conflito, não contam como membros das Forças Armadas. Contudo, se eles contribuírem, mesmo que minimamente, para o esforço militar ucraniano, provavelmente se tornarão alvos legítimos, ainda que temporariamente, para os militares russos. E não apenas no ciberespaço, mas potencialmente também no espaço físico (WATERMAN, 2023b).

Um princípio fundamental do Direito Internacional Humanitário diz que as Forças Armadas devem discriminar entre combatentes e não combatentes. Neste sentido, tais operações levantam a questão desafiadora do status legal, sob o DIH, dos membros do Exército de TI, tanto os hackers especialistas em TI, como os meros civis que se utilizam do *e-Vorog* para a coleta de inteligência operacional, ou daqueles que tiram fotografias de cadáveres com a finalidade de postar em redes sociais de parentes, com auxílio de IA.

3.1. Posição doutrinária do Comitê Internacional da Cruz Vermelha sobre o uso das novas tecnologias por civis em conflitos armados

Segundo o CICV (2024), os civis têm executado, há muito tempo, tarefas de apoio aos militares, no curso dos conflitos armados. Desta forma, com a digitalização das sociedades, algumas mudanças fundamentais ocorreram, não apenas nos tipos de operações que são conduzidas pelos civis, mas também no número de atores civis que participam dessas operações, em decorrência das características peculiares do ciberespaço que facilitam tal participação (CICV, 2024).

Neste caminho, para o CICV (2024) existem três principais tendências que podem representar riscos para os civis no contexto dos conflitos armados

da era contemporânea. Em primeiro lugar, um número sem precedentes de hackers civis têm conduzido operações cibernéticas e muitas vezes direcionam suas operações contra objetos civis. Em segundo lugar, a TI se apresenta aos beligerantes com novas ferramentas que podem encorajar os civis a apoiarem as operações militares, por exemplo, coletando informações militarmente relevantes por meio de seus smartphones, expondo assim os civis a ataques. Terceiro, quando empresas de tecnologia civis são contratadas para fornecer segurança cibernética e outros serviços de TI, para as forças armadas de partes em conflitos armados, existe risco real de que os ativos, a infraestrutura e os funcionários dessas empresas – que são, em princípio, civis – percam sua proteção legal contra os ataques direitos por estarem, supostamente, participando do esforço de guerra (CICV, 2024).

Desta forma, antes de aprofundar a análise sobre as condutas citadas na seção anterior, cabe enumerar a posição doutrinária do CICV, que foi formalizada em 2024, sobre a utilização da TI em conflitos armados. Desta forma, seguem as principais proposições jurídicas que estão presentes no relatório de 2024 (CICV, 2024):

1. Todos os Estados concordam que o direito internacional se aplica ao uso da TI. Neste caminho, os Estados também reconheceram, explicitamente, que, no contexto do uso da TI, "o direito internacional humanitário se aplica somente em situações de conflito armado", ressaltando que os princípios do DIH "de forma alguma legitimam ou encorajam o conflito" (UNGGE, 2021; UNGAR, 2021).[10] Estaproposição afirma o consenso de vários especialistas jurídicos, incluindo o CICV;[11]
2. As operações cibernéticas maliciosas podem interromper, desabilitar ou danificar fisicamente serviços e infraestrutura civis essenciais, instalações industriais, redes de comunicação, bancos de dados civis e outros setores civis da sociedade. Neste sentido, tais operações são capazes de ferir ou matar pessoas e colocar em risco a assistência àqueles que precisam;
3. Como a maioria das operações cibernéticas conduzidas em conflitos armados contemporâneos interrompem serviços, desabilitam computadores e redes ou danificam ou excluem dados sem causar danos físicos, interpretar o DIH à luz dessa realidade é fundamental;

[10] United Nations General Assembly (UNGA), Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (14 July 2021), para. 71(f); United Nations General Assembly, Resolution adopted on 8 December 2021 (A/RES/76/19), para. 2.

[11] For further discussion, see ICRC, "International humanitarian law and cyber operations during armed conflicts": Position paper, ICRC, Geneva, 2019, p. 4: <https://www.icrc.org/en/document/international-humanitarian-law-andcyber-operations-during-armed-conflicts>.

4. O CICV não concorda com a visão que considera um "ataque armado"[12] apenas as operações cibernéticas que são capazes de cruzar a fronteira do dano e produzir dano físico, semelhante ao causado pelos meios de guerra cinéticos. Pois, segundo esta visão a maioria das operações cibernéticas contra infraestrutura civil não seria restringida pelas regras mais detalhadas do DIH, que se originam nos princípios de distinção, proporcionalidade e precauções no ataque e proteção da população civil e objetos civis;
5. Para o CICV os dados são considerados "objeto", pois se não forem considerados como "objeto", dentro do sentido do que preconiza o DIH, a maioria das operações cibernéticas que danificam ou excluem dados civis não serão proibidas - o que seria um motivo de séria preocupação;
6. As operações cibernéticas militares não devem ser direcionadas contra objetos especificamente protegidos pelo Direito Internacional, tais como instalações médicas. Desta forma, ao se conduzir qualquer tipo de operação cibernética militar, deve-se tomar cuidado constante para poupar a população civil e os objetos civis. Portanto, direcionar operações cibernéticas disruptivas contra objetos civis, incluindo dados civis, ou ignorar seus efeitos incidentais sobre populações civis, seria incompatível com esta regra com o DIH;
7. Recorrer à perfídia aproveitando-se da TI com uso de *deepfake* é uma violação do DIH. Além disso, atos ou ameaças de violência,[13] cujo objetivo principal é espalhar o terror entre a população civil, são proibidos pelo DIH, inclusive ao usar *deepfakes*. Neste sentido, na condução de operações militares, incluindo operações de informação que fazem uso de *deepfakes*, as partes em conflito devem tomar cuidado constante para poupar a população civil, os civis e os bens civis;
8. Se indivíduos e grupos, incluindo os funcionários de empresas de tecnologia, conduzirem operações cibernéticas, no contexto de conflitos armados, eles devem cumprir os limites que o DIH estabelece para tais operações. Especificamente com relação a hackers civis operando no contexto de conflitos armados, esses limites foram resumidos em "8 Regras para Hackers Civis Durante a Guerra",[14] junto com quatro obrigações para os Estados garantirem o respeito a essas regras;

[12] For further discussion of the ICRC's views on the notion of 'attack' under IHL and the protection of data under IHL, see ICRC, "International humanitarian law and cyber operations during armed conflicts": Position paper, 2019, p. 7-8.

[13] BRASIL (1993), Art. 51(2); ICRC, Customary IHL Study, Rule 2.

[14] 8 Regras para Hackers Civis Durante a Guerra:
1. Não realizar ciberataques contra alvos civis;
2. Não utilizar malware ou outras ferramentas ou técnicas que se propaguem automaticamente e danifiquem indiscriminadamente alvos militares e alvos civis;

9. A coleta de informações militarmente relevantes por meio de smartphones ou outros dispositivos conectados e o fornecimento delas às forças armadas pode, em casos excepcionais, equivaler a "participação direta em hostilidades", o que significa que um civil perde sua proteção contra os ataques diretos se e enquanto esse for o caso;
10. O DIH exige que, em caso de dúvida,[15] em relação a uma conduta de uma pessoa ela deve ser considerada civil e protegida como tal. No entanto, o ato de encorajar civis a coletar informações militarmente relevantes leva ao risco de se colocar a população civil em risco em situação de perigo;
11. Para proteger civis e objetos civis de ataques ou danos incidentais, os Estados devem, sempre que possível, tentar segmentar – isto é, separar física ou tecnicamente – a infraestrutura de TIC (ou partes dela) que são usadas para fins militares daquelas que são utilizadas para fins civis; e
12. Mesmo que um beligerante conclua que um civil ou objeto civil perdeu a proteção legal contra os ataques direitos em virtude de seu envolvimento em operações cibernéticas ou de informação, o CICV apela aos beligerantes para que considerem cuidadosamente se será realmente necessário responder a tais ameaças com emprego de força cinética na busca de alcançar um propósito militar legítimo ou se outros meios ou métodos menos destrutivos (por exemplo, cibernéticos ou eletromagnéticos) podem ser usados para se atingir o mesmo efeito.[16]

3. Ao planear um ciberataque contra um alvo militar, fazer tudo o que for possível para evitar ou minimizar os efeitos que a sua operação possa ter sobre os civis;
4. Não conduzir qualquer operação cibernética contra instalações médicas e humanitárias;
5. Não conduzir qualquer ataque cibernético contra objetos indispensáveis à sobrevivência da população ou que possam libertar forças perigosas;
6. Não fazer ameaças de violência para espalhar o terror entre a população civil;
7. Não incitar a violações do direito internacional humanitário;
8. Cumprir estas regras mesmo que o inimigo não o faça. Quatro obrigações dos Estados para conter os piratas informáticos civis: 1) se os piratas informáticos civis agirem sob a instrução, direção ou controlo de um Estado, esse Estado é internacionalmente responsável por qualquer conduta desses indivíduos que seja incompatível com as suas obrigações jurídicas internacionais, incluindo o direito internacional humanitário (artigo 8º); 2) os Estados não devem encorajar civis ou grupos a agirem em violação do direito internacional humanitário; 3) os Estados têm a obrigação de agir com a diligência devida para impedir violações do direito internacional humanitário por piratas informáticos civis no seu território; e 4) os Estados têm a obrigação de processar os crimes de guerra e de tomar as medidas necessárias para suprimir outras violações do DIH. CICV, "Oito regras para os 'piratas informáticos civis' durante a guerra e quatro obrigações dos Estados para os impedir". Disponível em: <https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them>.

15 BRASIL (1993), Art. 50(1).

16 ICRC. *The Principles of Humanity and Necessity*, ICRC, Geneva. Disponível em: <https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/02_humanity_and_necessity-0.pdf>.

Percebe-se que a análise da mais nova visão do CICV sobre operações cibernéticas em conflitos armados se presta para revelar que, apesar da dificuldade conceitual que envolve a temática, bem como da escassez de costume internacional que aborde assertivamente todas as condutas que possam surgir no curso de um conflito armado, existe uma boa base doutrinária em construção pelo CICV, que é extremamente consistente com as regras postas do DIH.

Logo, isto pode ser um fator positivo para a persecução penal de crimes de guerra que possam ter sido, ou estar sendo praticados, pelo ciberespaço, no contexto da guerra da Ucrânia.

3.2 A análise jurídica da atuação de civis no conflito da Ucrânia

Já em relação ao DIH clássico, considerando as condutas realizadas por civis, expostas neste artigo, cabe ressaltar que as Convenções de Genebra estabelecem que os civis podem perder a proteção contra os ataques diretos, "enquanto participam diretamente das hostilidades" (PA I, 1977, Art. 51), mas o que isso significa exatamente ainda é muito discutido.

Estes civis poderiam ser alvos de ataques diretos das forças militares russas? Devem ser considerados combatentes? São membros de um grupo armado organizado ou são civis que participam diretamente das hostilidades? Quais seriam as implicações legais caso os membros do Exército de TI se juntassem, oficialmente, às Forças Armadas da Ucrânia, conforme intenciona o governo?

Segundo o direito de Genebra, são denominados "combatentes" as pessoas que, em um conflito armado internacional, possuem o privilégio de se envolver em hostilidades contra o inimigo e que, a menos que sejam especialmente protegidos por alguma circunstância especial (ferimento, rendição ou captura), podem ser objeto de ataque (BRASIL, 1993, PA I, 1977, Arts. 51–52).

Se capturados, eles têm direito o status de prisioneiro de guerra e imunidade de combatente (BRASIL, 1957, GC III, 1949, Art. 4º (A). Pelo que preconiza o DIH, a definição de civil é feita por oposição à definição de combate. Desta forma, se os membros do Exército de TI não são combatentes, consequentemente, serão civis.

De acordo com o Protocolo Adicional I de 1977 – Ucrânia e Rússia são partes em um conflito armado – e com o direito internacional consuetudinário, os civis são imunes a ataques diretos e protegidos de seus efeitos acidentais, pela proibição de realização de ataques com efeitos indiscriminados.

É da tropa atacante a obrigação de tomar precauções de segurança, antes e durante os ataques, bem como de respeitar o princípio da proporcionalidade e a regra de proporcionalidade (BRASIL, 1993, PA I, 1977, Arts. 51-52).

Biggerstaff (2023) afirma que existe pouca dificuldade em descobrir que os membros do Exército de TI devem ser considerados, atualmente, civis (pelo menos até que o governo ucraniano regularize a situação destes hackers).

As duas categorias clássicas de combatentes são estabelecidas nos Regulamentos anexos à Convenção IV de Haia, de 1907 (Art. 1º) e à III Convenção de Genebra, de 1949 (Arts. 4º (A) (1) – (2)), documentos amplamente considerados, que refletem o Direito Internacional costumeiro. Neste caminho, o Protocolo Adicional I vai consolidar estas duas normas em um único artigo (Art. 43 (1)).

O Art. 43, do PA I, vai aumentar um pouco mais o escopo e a amplitude da categoria de combatente, ao incluir:

1) membros das Forças Armadas (incluindo milícias ou corpos de voluntários que fazem parte deles) e
2) membros[17] de outras milícias ou corpos de voluntários "pertencentes a uma das partes beligerantes" (BRASIL, 1993, PA I, Art. 43).

A condição *sine qua non*, da primeira categoria, é que os indivíduos em questão, independentemente de suas funções, devem ser "formalmente" incorporados (ou seja, por meio de alistamento ou mecanismo similar respaldado pelo ordenamento jurídico do Estado) às Forças Armadas. E, segundo Biggerstaff (2023, p. 2 – tradução nossa), "esta é a condição que falta, atualmente, ao Exército de TI".

Para se enquadrar na segunda condição, o grupo ao qual uma pessoa pertence deverá preencher, coletivamente, várias condições.[18] Basta dizer que o Exército de TI falha em atender a esse requisito porque se trata de um grupo descentralizado, sem liderança designada, baseado na Internet, carecendo, por exemplo, de uma estrutura hierárquica organizada (BRASIL, 1993, PA I, art. 43; ICRC Comentário 1987 ao PA I, para. 1681) e de um Comandante,[19] capaz de fazer cumprir um sistema disciplinar interno. Consequentemente, "os mem-

[17] BRASIL (1993), Art. 1º (1) "grupos armados organizados que, sob a direção de um comando responsável, exerçam sobre uma parte desse território um controle tal que lhes permita realizar operações militares contínuas e concentradas e aplicar o presente Protocolo".

[18] "Artigo 43 – Forças Armadas – 1. As Forças Armadas de uma Parte em conflito compõem-se de todas as forças, grupos e unidades armados e organizados, colocados sob um comando responsável pela conduta de seus subordinados perante essa Parte, mesmo quando esta está representada por um governo ou por uma autoridade não reconhecidos por uma Parte adversa. Tais Forças Armadas deverão estar submetidas a um regime de disciplina interna que as faça cumprir, *interalia*, as normas de Direito Internacional aplicáveis aos conflitos armados. 2. Os membros das Forças Armadas de uma Parte em conflito (exceto aqueles que são parte do pessoal sanitário e religioso a que se refere o Artigo 33 da Terceira Convenção) são combatentes, isto é, têm direito a participar diretamente das hostilidades. 3. Sempre que uma Parte em conflito incorpore às suas Forças Armadas um organismo paramilitar ou um serviço armado encarregado de velar pela ordem pública, deverá notificá-lo as outras partes em conflito" (BRASIL, 1993, PA I, art. 43; ICRC Comentário 1987 ao PA I, para. 1681).

[19] Comentário do CICV 2020 ao GC III, para. 1013-14; CICV 1987 Comentário ao PA I, para. 1672.

bros do Exército de TI são civis, pelo menos por enquanto" (BIGGERSTAFF, 2023, p. 2 – tradução nossa).

Ressalta-se também que a qualificação de um indivíduo como civil, para o escopo de proteção do DIH, não significa que sua imunidade aos ataques diretos se aplica em *todas as circunstâncias.*

Para Biggerstaff (2023), os atuais membros do Exército de TI podem perder essas proteções, temporariamente, quando engajados em hostilidades cibernéticas. Igualmente seria para qualquer civil que estivesse coletando inteligência operacional para atribuir algum tipo de vantagem para uma das partes. Isto configura o "nexo beligerante", um dos quesitos que caracterizam uma participação direta de um civil nas hostilidades.

Desta forma, é fundamental que se faça a diferenciação de civis agindo de forma individual ou desorganizada, daqueles que são membros de grupos não estatais, que estão devidamente autorizados pelo Estado (de forma tácita ou expressa).

Em tese, para as ações cinéticas da guerra real, civis somente perdem suas proteções contra os ataques diretos "enquanto" participarem diretamente das hostilidades (BRASIL, 1993, PA I, art. 51(3)). Entretanto, existe uma controvérsia entre a visão do CICV e a visão do Manual de Tallinn 2.0. Para o Manual de Tallinn 2.0, não existem interrupções na perda da proteção (SCHMITT, 2017). Desde as primeiras ações exploratórias, até a verificação do êxito da operação cibernética maliciosa, o hackercivil, participante da ação hostil, pode ser alvo de ataques diretos, inclusive ataques cinéticos.

Sob uma abordagem mais restritiva, sugerida pelo CICV, em sua "Orientação Interpretativa sobre a Noção de Participação Direta em Hostilidades", apenas aqueles indivíduos com uma "função de combate contínua" – em contraste com os indivíduos que possuem "funções exclusivamente políticas, administrativas ou outras funções não relacionadas ao combate" (MELZER, 2009, p. 33-34 – tradução nossa) – podem ser atacados da mesma maneira que os combatentes são. Indivíduos que não atuam em tal capacidade seriam "passíveis de serem atacados apenas quando participam diretamente das hostilidades" (BIGGERSTAFF, 2023, p. 2 – tradução nossa).

Ao avaliar se o Exército de TI se qualificaria como um grupo armado não estatal, no contexto da guerra cibernética, a orientação sugerida pelo Grupo Internacional de Especialistas (GIE), no Manual de Tallinn 2.0, sobre o Direito Internacional Aplicável às Operações Cibernéticas é bastante instrutiva. Considera-se que tal grupo está "armado" se ele tiver a capacidade de realizar ataques cibernéticos. Entende-se que é "organizado" se ele estiver sob uma estrutura de Comando estabelecida e puder conduzir operações militares autossustentadas.

Operações cibernéticas, incluindo campanhas secretas de espionagem, levam meses para serem preparadas e montadas, mas podem ser facilmente interrompidas, por exemplo, por meio de um ataque hacktivista, grosseiro e inoportuno, que pode alertar e colocar os defensores cibernéticos do inimigo em alerta máximo.

Desta forma, Waterman (2023b) acredita que, apesar da ausência de uma liderança visível e centralizada, as ações do Exército de TI são coordenadas de uma forma peculiar e diferente, talvez por meio de uma linguagem que somente os hackers consigam compreender com facilidade. Eles recrutaram esse Exército de TI, que está espalhado por todo o mundo e, provavelmente, não está agindo sob as ordens de alguém, mas encontrando oportunidades e explorando-as (WATERMAN, 2023b).

A extensão da organização não precisa, necessariamente, atingir o nível de uma unidade disciplinada militar convencional. No entanto, as operações cibernéticas maliciosas isoladas, por parte de particulares, não são suficientes para atender este requisito, segundo a visão do Manual (SCHMITT, 2017b, regra 83, parágrafo 11). Mesmo pequenos grupos de hackers, provavelmente, não atenderão ao requisito de organização. Desta forma, a organização ou não de um determinado grupo deve ser determinada caso a caso, incluindo-se os civis que executam tarefas fora do escopo do Exército de TI, mas que contribuam para uma vantagem a uma das partes.

Percebe-se que, pela abordagem do Manual de Tallinn 2.0, existem poucas dúvidas de que o Exército de TI se caracterizaria como um grupo armado não estatal. Entretanto, até que seja legalmente reconhecido, não existe tanta certeza de que ele esteja suficientemente organizado. Embora os detalhes na mídia sejam limitados, alguns relatos podem servir para caracterizar, amplamente, a existência do grupo. Este se ativa em torno de postagens no *Twitter*, visivelmente organizado e liderado por um *chat*, no canal do *Telegram* – como um amálgama "descentralizado", que reúne seus membros mediante chamado, muitos dos quais só se associam por meio da Internet.

Tendo em vista tais descrições, e sem detalhes mais específicos sobre a estrutura e organização do Exército de TI, não é muito fácil classificar o referido "exército" como um grupo armado não estatal. Todavia, caso seja realmente editada uma lei para sua "oficialização" como grupo pertencente ao Estado ucraniano, sua classificação ficará inequívoca: o primeiro grupo armado não estatal, no contexto da guerra cibernética, a ser empregado em um conflito armado real. Caso contrário, a Rússia pode atacar, mesmo de forma cinética, separadamente, os indivíduos cujos atos específicos, caso a caso, constituam, pelo entendimento do CICV como uma participação direta de civis nas hostilidades (BIGGERSTAFF, 2023). Entretanto, a Rússia deverá ter atenção para as regras da neutralidade, sob pena de arrastar algum outro Estado para o conflito.

O CICV diz que a participação direta deve envolver ações que afetem, deliberadamente, as operações militares em favor de um dos lados. Isto, para Joshi (2023) é uma exigência muito alta. Os especialistas concordam que os civis que apenas respondem a perguntas feitas por militares, em relação ao inimigo, não atingem o limite. Além disso, a maior parte da inteligência transmitida por aplicativos é "muito geral ou insignificante para atingir o limite do critério de dano", argumenta Macak (MACAK, 2023 – tradução nossa).

Um civil teria que coletar e transmitir informações "como parte de uma operação coordenada para fins de um ataque específico" (MACAK, 2023 – tradução nossa), mas quem deve saber se o dado operacional é ou não útil para uma determinada operação militar é o analista de inteligência, em uma fase posterior à coleta do dado. Neste caso, a participação do civil já estaria configurada. Entretanto, não resta dúvida de que pilotar um drone para corrigir o fogo de artilharia certamente se qualificaria como uma participação direta de civil nas hostilidades (JOSHI, 2023).

Não existe um consenso estabelecido no DIH (convencional ou costumeiro) sobre quais atos, se desempenhados por um civil, poderiam se qualificar para a caracterização do agente como participando diretamente das hostilidades ativas de um conflito armado. Apesar de não existir um posicionamento pacífico na doutrina, a "Orientação Interpretativa Normativa do CICV", que trata do tema, sugere que três "elementos constitutivos devem estar presentes" (MELZER, 2009, p. 46 – tradução nossa): um limite razoável de dano empreendido pela conduta, uma relação de causa e efeito entre a conduta e o resultado e um nexo beligerante que indique uma intenção clara de se oferecer uma vantagem a uma parte beligerante em detrimento da outra.

Estes requisitos, da forma como foram idealizados, não seriam difíceis de serem analisados em casos de conflitos armados reais no mundo físico, uma vez que, em sua maioria, estão relacionados com a fisicalidade do fenômeno político-social que é a guerra. Entretanto, em se tratando de ações (condutas) na esfera da existência humana e também do direito tão peculiares e únicas, como são caracterizadas as operações cibernéticas, deve-se ter cuidado especial quanto à realização da transposição dos conceitos relacionados ao instituto jurídico da "participação direta de civis em hostilidades".

Tudo isto sob o risco de desconsiderar a relevância da disrupção – que está relacionada com a pós-territorialidade –, a ausência de fisicalidade e a importância que possui para a compreensão do fenômeno jurídico, sob os olhos da tecnologia e da inovação. Dada a natureza das operações cibernéticas e dos recursos modernos, essas questões em aberto podem ter poucas consequências práticas para o Exército de TI. Independentemente de onde esteja a linha, uma vez que um membro do Exército de TI cesse permanentemente sua participa-

ção direta, "ele não poderá ser mais alvo das forças russas" (BIGGERSTAFF, 2023, p. 3).

Em relação a outra questão controversa, que envolve o DIH, a publicação das fotos de cadáveres, ou restos mortais de combatentes inimigos, implica que tal prática viola o Artigo 13 da terceira Convenção de Genebra, o qual versa sobre o trato com prisioneiros de guerra e estabelece que estes "devem sempre ser tratados com humanidade" e "protegidos, particularmente contra atos de violência ou intimidação e contra insultos e curiosidade pública" (BRASIL, 1957, GC III, Art. 13). De acordo com adoutrina[20] do DIH, divulgar publicamente a fotografia de um soldado inimigo é humilhante e, portanto, estritamente proibido (BIGGERSTAFF, 2022). Entretanto, Biggerstaff (2023), em um exame mais minucioso, acredita que a afirmação de violação não se sustenta, porque o Artigo 13 não se aplica aos restos mortais do inimigo encontrados no campo de batalha, sob o fundamento de que as proteções da GC III se aplicam apenas a soldados "que caíram em poder do inimigo" (BRASIL, 1957, GC III, Art. 4º), ou seja, prisioneiros de guerra, não restos mortais encontrados no campo de batalha.

Quanto à questão da notificação familiar, os procedimentos[21] estabelecidos pela Convenção referem-se apenas àqueles "que morrem como prisioneiros de guerra" e "prisioneiros de guerra que morreram em cativeiro" (BRASIL, 1957, GC III, Art. 4º), posição com a qual o autor do presente trabalho não concorda, pois "restos mortais" que possibilitem identificação por biometria facial devem merecer especial atenção e proteção jurídica diferenciada de simples restos humanos de cadáveres, principalmente pelas consequências jurídicas e psicológicas que tal postura gera no mundo real. O DIH estabelece procedimentos[22] especiais para o trato com militares mortos em combate, independentemente de estarem ou não na condição de prisioneiros de guerra. Exemplo disto é a proibição de violação de navios de guerra afundados em combate, por serem considerados túmulos de combatentes.

---

[20] Ver Comitê Internacional da Cruz Vermelha (CICV), Comentário de 2020, para. 1624.

[21] Artigo 120; ver também Artigo 122; Comentário do CICV 2016 ao GC I, para. 1350.

[22] O DIH relevante ao caso é encontrado em GC I. O Artigo 15 exige que as partes "procurem os mortos e evitem que sejam despojados". Uma vez encontrados os restos mortais, os seus depositários devem criar um registo contendo dados de identificação e outros dados administrativos que devem ser encaminhados, juntamente com os bens pessoais do falecido, para um "Gabinete de Informação" nacional (GC I, 1949, Art. 16). Os Gabinetes de Informação são entidades oficiais criadas por cada parte que fazem a ligação e coordenam o trato com os desaparecidos e mortos em ação através da Agência Central de Rastreamento, que se trata de uma organização intermediária neutra gerida pelo CICV, para a transferência de informações e efeitos entre partes hostis sobre prisioneiros e soldados mortos (GC III, 1949, Arts. 122 e 123). Assim que a Agência Central de Rastreamento encaminhar informações da parte sob custódia, o Bureau de Informações do soldado falecido deve notificar os parentes mais próximos (GC I, 1949, Art. 16). Consulte também o Comentário do CICV 2016 ao GC I, para. 1599 e a GC III, Art. 123.

Retomando o Direito Internacional Consuetudinário, uma das regras mais antigas no Direito da Guerra é a de tratar os restos mortais de soldados mortos com respeito. Embora o respeito seja um termo vago e eminentemente subjetivo, o tratamento desrespeitoso normalmente requer atos de indignação específicos cometidos contra ou com cadáveres. A Regra 113 (Tratamento dos Mortos) do estudo de Direito Internacional Consuetudinário do CICV, por exemplo, afirma: "Cada parte no conflito deve tomar todas as medidas possíveis para evitar que os mortos sejam espoliados. A mutilação de cadáveres é proibida" (HENCKAERTS; BECK, 2005). Ademais, segundo Biggerstaff (2023), a especificidade da regra implicaria que apenas atos que atendam a um "certo limite de desrespeito" são proibidos, entretanto, qual o grau de subjetividade aceitável para se definir o que seria "certo limite de desrespeito"?

Evitar que sofrimento desnecessário seja causado contra civis é um dos principais paradigmas de sustentação do DIH, o que se estende também para famílias que sejam alvo de guerras psicológicas, as quais visam alcançar objetivos políticos mais amplos. Não se pode aceitar tal prática como algo legal e legítimo, pois no mínimo, fere princípios éticos mais básicos, como também o princípio jurídico da humanidade. A referida postura é consistente com a criminalização dos maus-tratos aos mortos que existe no Direito Penal Internacional. Neste sentido, o Artigo 8º (2) (b) (xxi), do Estatuto de Roma, por exemplo, proíbe atos humilhantes, degradantes ou que causem indignação contra cadáveres "de tal grau que sejam geralmente reconhecidos como um ultraje à dignidade pessoal" (BRASIL, 2002).

A Ucrânia está violando o processo descrito na GC I para notificar familiares de militares inimigos mortos em combate. Segundo a situação em curso, as forças militares da Ucrânia, bem como o Exército de TI, estão entrando em contato com familiares, pelas mídias sociais, de forma abrupta e ilegal sem usar a Agência Central de Rastreamento do CICV como intermediária, conforme os moldes preconizados pelas normas. Tal conduta é, sem dúvida, uma grave violação técnica do GC I, Artigo 16, que tem o potencial de ensejar a responsabilização do Estado ucraniano por cometer um ato ilícito na esfera internacional, bem como a responsabilização penal internacional individual dos civis e ou militares que estão realizando a conduta ilícita, quer estejam ou não agindo em nome da Ucrânia.

Vale lembrar que civis que participam diretamente de hostilidades estão sujeitos à detenção pelo Estado inimigo. Para que a prisão seja efetuada de forma correta, deve-se respeitar o status relacionado à conduta do civil e ao momento do conflito que tal conduta é realizada. Neste sentido, caso o civil seja detido durante a realização de um ato que configure uma participação direta nas hostilidades, de forma isolada de um grupo armado não estatal, sua de-

tenção se dará sob os paradigmas jurídicos penais da jurisdição territorial do local da prisão, e, neste caso, não existe imunidade de combatente, respondendo integralmente pelos crimes que tiver cometido com o ato de participação. Tal situação somente se modificará caso o civil pertença a um grupo armado não estatal autorizado pelo Estado, segundo o procedimento preconizado no DIH.

4 Considerações finais

Os conflitos armados do século XXI englobam muita tecnologia, no que diz respeito aos métodos e meios de combate. A chamada "guerra cibernética" já está incorporada como arma tática ou estratégica.

Desta forma, em decorrência das características peculiares do ciberespaço, indivíduos que não possuem prerrogativas que os combatentes regulares possuem têm buscado novas formas de participação diretas nas hostilidades cibernéticas.

A inclusão de civis em hostilidades ativas de um conflito armado influencia, de forma contundente, o status de proteção construído pelo Direito Internacional Humanitário para a proteção de pessoas que não participem das ações de guerra. A participação de civis em hostilidades no curso de conflitos armados não se traduz em algo novo para os estudos militares estratégicos, entretanto, o ciberespaço permite que tal participação seja realizada em larga escala, de forma quase anônima e a grandes distâncias do teatro de operações.

A inserção indiscriminada de civis em ações diretas de combate gera grande dificuldade para a investigação, processamento e persecução penal das condutas que possam ultrapassar o limite da legalidade. Tal dinâmica exige abordagem assertiva e direta da estrutura jurisdicional do Estado nacional que for vítima de tais condutas.

Por um lado, o Estado deve tomar as precauções para legalizar, conforme sua lei nacional, a utilização de milícias digitais em conflitos armados e por outro deve evitar que civis tomem parte de conflitos cibernéticos. O ato de incentivar que pessoas comuns sejam expostas às graves consequências dos conflitos armados poderá gerar responsabilização objetiva para o Estado nas lides internacionais.

A democratização da participação direta em conflitos armados, de forma alguma, poderá incentivar a violação de direitos humanos consagrados e o enfraquecimento do princípio da proteção internacional da pessoa humana.

Referências

BASSO, D. French army hails Ukraine's cyber defence 'revolution'. *Euractivi*, Brussels, 2023. Disponível em: <https://www.euractiv.com/section/politics/news/french-army-hails-ukraines-cyber-defence-revolution/>. Acesso em: 25 jul. 2023.

BIGGERSTAFF, W. C. The status of Ukraine's "IT Army" under the Law of Armed Conflict. *Lieber Institute. West Point*. New York, 2023. Disponível em: <https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/>. Acesso em: 25 jul. 2023.

_____ . Ukraine Symposium – photos of the dead. *Lieber Institute. West Point.* New York, 2022. Disponível em: <https://lieber.westpoint.edu/photos-of-dead/>. Acesso em: 25 jul. 2023.

BRASIL. *Decreto nº 4.388 de 25 de setembro de 2002.* Promulga o Estatuto de Roma do Tribunal Penal Internacional. Brasília: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2002/d4388.htm>. Acesso em: 25 jul. 2023.

_____ . *Decreto nº 42.121, de 21 de agosto de 1957.* Promulga as Convenções concluídas em Genebra, a 12 de agosto de 1949, destinadas a proteger as vítimas da guerra. Rio de Janeiro: Independência da República, 1957. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1950-1969/D42121.htm>. Acesso em: 25 jul. 2023.

_____ . *Decreto nº 849, de 25 de junho de 1993.* Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados. Brasília: Independência da República, 1993. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0849.htm>. Acesso em: 25 jul. 2023.

BREWSTER, T. Ukraine Starts Using Facial Recognition To Identify Dead Russians And Tell Their Relatives. *Forbes*, Jersey City, 2022. Disponível em: <https://www.forbes.com/sites/thomasbrewster/2022/03/23/ukraine-starts-using-facial-recognition-to-identify-dead-russians-and-tell-their-relatives/?sh=f5b58ac28985>. Acesso em: 25 jul. 2023.

CRIMES Committed during a Full-scale Invasion of the Russian Federation. *Office of the Prosecutor General:* official web portal, [S.l.], 2022. Disponível em: <https://www.gp.gov.ua/>. Acesso em: 21 jun. 2022.

CRIMES Committed during a Full-scale Invasion of the Russian Federation. (*Official website of the Office of the Prosecutor General:* official web portal). EUROPEAN Parliament resolution of 23 November 2022 on recognising the Russian Federation as a state sponsor of terrorism.

HARWELL, D. Ukraine is scanning faces of dead Russians, then contacting the mothers. *The Washington Post*, Washington, 2022. Disponível em: <https://www.washingtonpost.com/technology/2022/04/15/ukraine-facial-recognition-warfare/>. Acesso em: 25 jul. 2023.

HENCKAERTS, J. M.; BECK, L. D. *Direito Internacional Humanitário Consuetudinário.* Cambridge: Cambridge University Press, 2005, regras 1-11, 12, 14, 15, 17, 24, Volume I e II: Regras. Disponível em: <https://www.icrc.org/sites/default/files/topic/file_plus_list/direito_internacional_humanitario_consuetudinario.pdf>. Acesso em: 23 jul. 2023.

ICRC. International Humanitarian Law Databases. Comentário do CICV 2020 ao GC III, para. 1.013-1.014. *Geneva Convention (III) on prisioners of war*, Geneva, 2020. Disponível em: <https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-4/commentary/2020?activeTab=undefined>. Acesso em: 23 jun. 2023.

_____ . “8 rules for “civilian hackers” during war, and 4 obligations for states to restrain them”. Disponível em: <https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them>. Acesso em: 25 jul. 2023.

_____ . “International humanitarian law and cyber operations during armed conflicts”: Position paper. *ICRC*, Geneva, 2019, p. 4. Disponível em: <https://www.icrc.org/en/document/international-humanitarian-law-andcyber-operations-during-armed-conflicts>. Acesso em: 25 jul. 2023.

_____ . Fair Trial Guarantees. IHL Databases. Available at. Access on: July 5, 2023; Article 85(4)(e) Protocol Additional (I) to the Geneva Conventions of 12 August 1949 and relating to the protection of victims of international armed conflicts.

_____ . The Principles of Humanity and Necessity. *ICRC*, Geneva. Disponível em: <https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/02_humanity_and_necessity-0.pdf>. Acesso em: 25 jul. 2023.

ICRC-REPORT. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. *34º International Conference on the Red Cross.* Geneve. 2024. Available at: <34IC_10.6-IHL-Challenges-Report-EN.pdf>. Acesso em: 25 jul. 2023.

JOSHI, S. Battlefield Lessons-Special Report. *The Economist*, New York, 2023. Disponível em: <https://www.economist.com/special-report/2023/07/03/technology-is-deepening-civilian-involvement-in-war>. Acesso em: 25 jul. 2023.

KILOVATY, I. Virtual Violence. Disruptive Cyberspace Operations as “Attacks” Under Humanitarian Law. *Michigan Telecommunications nad Technology Law Review*, Michigan, v. 23, n. 1, 2016. Disponível em: <https://repository.law.umich.edu/mttlr/vol23/iss1/3>. Acesso em: 22 set. 2023.

KOWALCZEWSKA, Kaja. War-Torn Justice: Empirical Analysis of the Impact of Armed Conflict on Fair Trial Guarantees in Ukraine. *Rev. Bras. de Direito Processual Penal*, Porto Alegre, v. 9, n. 3, p. 1.061-1.107, set.-dez. 2023. Disponível em: War-Torn Justice: Empirical Analysis of the Impact of Armed Conflict on Fair Trial Guarantees in Ukraine – Dialnet. Acesso em: 25 jul. 2023.

KUIBIDA, Roman, MOROZ, Liana and SMALIUK, Roman, “Justice in the East of Ukraine During the Ongoing Armed Conflict” (2020) 11(2) *International Journal for Court Administration* 9. DOI: <https://doi.org/10.36745/ijca.34>. Acesso em: 25 jul. 2023.

LONAS, L. Ukraine has used facial recognition tech to notify hundreds of Russian families of dead soldiers: report. *The Hill*, Washington, 2022. Disponível em: <https://thehill.com/policy/international/3269911-ukraine-has-used-facialrecognition-tech-to-notify-hundreds-of-russian-families-of-dead-soldiers-report/>. Acesso em: 25 jul. 2023.

MACAK, K. Civilianization of Digital Operations: A Risky Trend. *Lawfare*, [S.l.], 2023. Disponível em: <https://www.lawfaremedia.org/article/civilianization-digital-operations-risky-trend>. Acesso em: 25 jul. 2023.

MELZER, N. Of The Red Cross, Interpretive Guidance On The Notion Of Direct Participation In Hostilities Under International Humanitarian Law. *Int’l Comm.* Geneva: International Committee of the Red Cross, 2009. Disponível em: <https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf>. Acesso em: 25 jul. 2023.

REPORT of the Independent International Commission of Inquiry on Ukraine, United Nations Human Rights Council, 3023; Emergency in Ukraine: external situation report.

RESOLUTION 49/1. Situation of human rights in Ukraine stemming from the Russian aggression.

RESOLUTION ES-11/1. Aggression against Ukraine.

RESOLUTION. Principles of the Charter of the United Nations underlying a comprehensive, just and last ing peace in Ukraine.

REUTERS. "It was a massacre": Mariupol residents recall battle for Ukrainian city, 2022.

ROMANDASH, A. Ukraine's IT Army: Digital Resistance to Russian Propaganda. In: O'Brien, J. *Peace Policy:* Solutions to Violent Conflict, May 2023. Notre Dame: Kroc Institute for International Peace Studies, 2023. Disponível em: <https://doi.org/10.7274/qr46qz24c90>. Acesso em: 23 jul. 2023.

SCHMITT, M. N. Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge: Cambridge University Press, 2017. Disponível em: <https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf>. Acesso em: 25 fev. 2023.

SCOTT, M. How Ukraine used Russia's digital playbook against the Kremlin. *Politico*, [S.l.], 2022. Disponível em: <https://www.politico.eu/article/ukraine-russia-digitalplaybook-war/>. Acesso em: 25 jul. 2023.

SHELEST, H. Defend. Resist. Repeat: Ukraine's lessons for European defence. *The European Council on Foreign Relations*, London, 2022, p. 2 – tradução nossa. Disponível em: <https://ecfr.eu/publication/defend-resist-repeat-ukraines-lessons-for-european-defence/>. Acesso em: 25 jul. 2023.

SHORE, J. Don't Underestimate Ukraine's Volunteer Hackers. *Foreign Policy*, Washington, 2022. Disponível em: <https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/>. Acesso em: 25 jul. 2023.

SOESANTO, S. The IT Army of Ukraine Structure, Tasking, and Ecosystem. ETH Zürich: Cyberdefense Report Center for Security Studies (CSS). *ETHzürich*, Zürich, 2022. Disponível em: <css.ethz.ch/en/publications/risk-and-resilience-reports.html>. Acesso em: 25 jul. 2023.

THE ECONOMIST. How a chatbot has turned Ukrainian civilians into digital resistance Fighters. *The Economist*, [S.l.], 2023. Disponível em: <https://www.economist.com/the-economist-explains/2023/02/22/how-a-chatbot-has-turned-ukrainian-civilians-into-digital-resistance-fighters>. Acesso em: 25 jul. 2023.

UNGA – United Nations General Assembly. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (14 July 2021), para. 71(f); United Nations General Assembly, Resolution adopted on 8 December 2021 (A/RES/76/19), para. 2.

WATERMAN, S. Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army. *Newsweek*, New York, 2023a. Disponível em: <https://www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814>. Acesso em: 25 jul. 2023.

_____ . Ukraine's Volunteer Cyber Army Could Be Blueprint for the World. *Experts Newsweek 90*, New York, 2023b. Disponível em: <https://www.newsweek.com/ukraine-war-cyber-army-attack-strategy-warfare-1780970>. *Acesso em: 25 jul. 2023*.